PN - JP2001111538 A 20010420
PD - 2001-04-20
PR - JP19990284245 19991005
OPD - 1999-10-05
TI - COMMUNICATION SYSTEM, METHOD THEREFOR, COMMUNICATION EQUIPMENT AND IC CARD
IN - YAMADA MASANARI
PA - DAINIPPON PRINTING CO LTD
IC - H04L9/08 ; G09C1/00 ; H04L9/32

TI - Communication system has transmitter which transmits authenticated electronic certificate acquired from authentication station to gateway for updating disclosure key in IC card
PR - JP19990284245 19991005
PN - JP2001111538 A 20010420 DW200139 H04L9/08 009pp
PA - (NIPQ) DAINIPPON PRINTING CO LTD
IC - G09C1/00 ;H04L9/08 ;H04L9/32
AB - JP2001111538 NOVELTY - Encryption processor encrypts disclosure key which is signed with secret key inside IC card (40), and outputs encrypted key using secret key. The encrypted key before being output is sent to authentication station (30). Authenticated electronic certificate is acquired from the station and is transmitted by transmitter (10) to gateway (20), so as to update the disclosure key in the IC card.
- DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
- (a) Communication procedure;
- (b) Communication apparatus;
- (c) IC card
- USE - For performing communication of high secret certificates using open networks such as internet.

4

- ADVANTAGE - Ensures highly secure and reliable communication of electronic certificates using open networks such as internet.
- DESCRIPTION OF DRAWING(S) - The figure shows the communication system. (Drawing includes non-English language text).
- Transmitter 10
- Gateway 20
- Authentication station 30
- IC card 40
- (Dwg.1/3)

OPD - 1999-10-05

AN - 2001-372143 [39]

PN - JP2001111538 A 20010420

PD - 2001-04-20

AP - JP19990284245 19991005

IN - YAMADA MASANARI

PA - DAINIPPON PRINTING CO LTD

TI - COMMUNICATION SYSTEM, METHOD THEREFOR, COMMUNICATION EQUIPMENT AND IC CARD

AB - PROBLEM TO BE SOLVED: To provide communication with high reliability in which no private key can be taken out, not even by a network manager.

- SOLUTION: In a gateway10, an RSA key is generated in an IC card40 and a public key is signed using the private key which is used inside the IC card40 at present. The gateway 10 transmits the signed public key to a certifying authority 30. In the certifying authority30, the transmitted public key is inspected using the present public key of the gateway10, a new public key is acquired, singed by a private key of the certificate authority 30 and is transmitted to the gateway10 as an electronic certificate. The gateway10 transmits the electronic certificate to a desired communicating destination such as a gateway20 and

updates the key. In the gateway10, security is enhanced, since no private key is taken out of the IC card40 by enciphering communication in the IC card40, by using the private key held in the IC card40.

- H04L9/08 ;G09C1/00 ;H04L9/32

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－111538
（P2001－111538A）
(43)公開日　平成13年４月20日(2001.4.20)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０９Ｃ　1/00	６４０Ｂ　５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０		６６０Ａ
	６６０	Ｈ０４Ｌ　9/00	６０１Ｚ
Ｈ０４Ｌ　9/32			６０１Ｆ
			６７５Ｄ

審査請求　未請求　請求項の数９　ＯＬ　（全９頁）

(21)出願番号　特願平11－284245

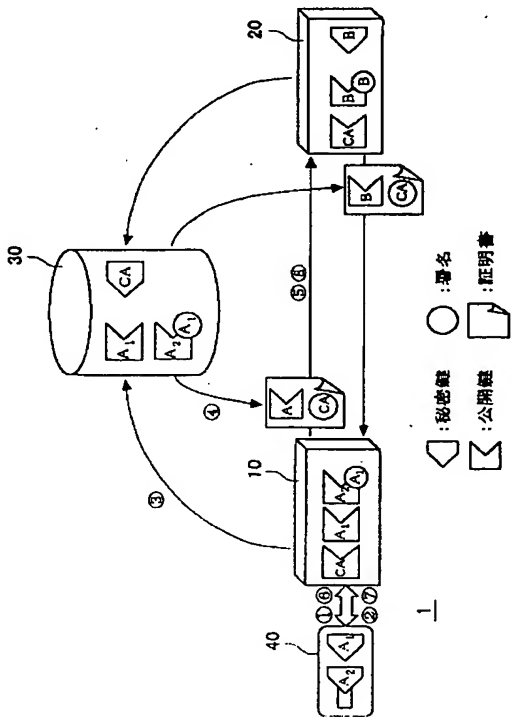
(22)出願日　平成11年10月５日(1999.10.5)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　山田　真生
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(74)代理人　100094053
弁理士　佐藤　隆久

Ｆターム(参考)　5J104 AA16 EA05 EA19 JA28 LA03
LA06 MA01 NA02 NA35 NA37
PA07

(54)【発明の名称】　通信システムとその方法、通信装置およびＩＣカード

(57)【要約】
【課題】ネットワーク管理者でも秘密鍵を取り出すことができない、信頼性の高い通信を提供する。
【解決手段】ゲートウェイ１０では、ＩＣカード４０内でＲＳＡ鍵を生成し、ＩＣカード４０内部で現在使用している秘密鍵により公開鍵に署名を行なう。この署名された公開鍵を、ゲートウェイ１０は認証局３０に送る。認証局３０では、ゲートウェイ１０の現在の公開鍵を用いてこれを検査し、新たな公開鍵を獲得し、これに認証局３０の秘密鍵で署名をし、電子証明書としてゲートウェイ１０に送信する。ゲートウェイ１０は、この電子証明書をゲートウェイ２０など所望の通信先に送信し、鍵の更新を行なう。ゲートウェイ１０では、通信文もＩＣカード４０内でＩＣカード４０内に保持されている秘密鍵を用いて暗号化することにより、秘密鍵は一切ＩＣカード４０外部に出ず、セキュリティ性が高まる。



【特許請求の範囲】

【請求項１】複数のノードおよび認証局が、必要に応じて相互の公開鍵を保持し、公開鍵方式に基づいた暗号文を用いて相互に通信を行なう通信システムであって、
前記ノードの少なくとも１つのノードは、
公開鍵および秘密鍵を有する公開鍵対を内部で生成し、秘密鍵は内部で外部よりアクセス不可能に保持し、生成した公開鍵を、以前に生成し内部に保持されている秘密鍵を用いて暗号化し出力する暗号処理装置と、
前記暗号処理装置より出力された以前の秘密鍵を用いて暗号化された生成された公開鍵を、前記認証局に送信し、前記生成された公開鍵に前記認証局が認証を行なった電子証明書を獲得する電子証明書獲得手段と、
前記獲得した電子証明書を、通信先のノードに送信し、公開鍵の更新を行なう送信手段とを有する通信システム。

【請求項２】複数のノードおよび認証局が、必要に応じて相互の公開鍵を保持し、公開鍵方式に基づいた暗号文を用いて相互に通信を行なう通信方法であって、
前記ノードの少なくともいずれかのノードにおいて、外部より任意にアクセス不可能な装置であって、公開鍵および秘密鍵を有する公開鍵対を内部で生成し、秘密鍵は内部で外部よりアクセス不可能に保持し、少なくとも生成した公開鍵を以前に生成し内部に保持されている使用中の秘密鍵を用いて暗号化し出力する暗号処理装置を用いて、使用中の秘密鍵を用いて暗号化された新たな公開鍵データを生成し、
前記暗号化された新たな公開鍵データを前記認証局に送信し、
前記認証局は、送信された前記暗号化された新たな公開鍵データを復号化して、該新たな公開鍵データを獲得し、
前記獲得した新たな公開鍵データに当該認証局の秘密鍵を用いて認証を行ない、
前記認証を行なった公開鍵データを当該公開鍵データの送信元のノードに送信し、
当該送信元のノードは、前記認証局の認証の得られた公開鍵データを、通信先の任意のノードに送信し、
前記認証局の認証の得られた公開鍵データが送信されたノードは、前記認証局の公開鍵を用いて前記認証の検査を行ない、前記新たな公開鍵を獲得し、
前記送信元のノードと他のノードおよび認証局は、前記獲得された新たな公開鍵を用いて前記通信を行なう通信方法。

【請求項３】前記送信元のノードは、任意のデータを送信する際には、当該データを前記暗号処理装置に入力し、当該暗号処理装置内において該データを前記内部に保持されている使用中の秘密鍵を用いて暗号化し、当該暗号化したデータを送信先に送信する請求項２に記載の通信方法。

【請求項４】複数のノードおよび認証局が、必要に応じて相互の公開鍵を保持し、公開鍵方式に基づいた暗号文を用いて相互に通信を行なう通信システムにおいて、前記ノードとして用いられる通信装置であって、
公開鍵および秘密鍵を有する公開鍵対を内部で生成し、秘密鍵は内部で外部よりアクセス不可能に保持し、生成した公開鍵を、以前に生成し内部に保持されている秘密鍵を用いて暗号化し出力する暗号処理装置と、
前記暗号処理装置より出力された以前の秘密鍵を用いて暗号化され生成された公開鍵を、所望の通信先に送信する通信手段とを有する通信装置。

【請求項５】前記通信手段は、前記暗号処理装置より出力された以前の秘密鍵を用いて暗号化され生成された公開鍵を、まず前記認証局に送信し、前記生成された公開鍵に前記認証局が認証を行なった電子証明書を獲得し、さらに、前記獲得した電子証明書を、所望の通信先のノードに送信する請求項４に記載の通信装置。

【請求項６】送信対象のデータを前記暗号処理装置に入力する入力手段をさらに有し、
前記暗号処理装置は、前記入力される送信対象のデータを、前記以前に生成し内部に保持されている秘密鍵を用いて暗号化し出力し、
前記通信手段は、さらに、前記出力された暗号化された送信対象のデータを、所望の通信先のノードに送信する請求項５に記載の通信装置。

【請求項７】前記暗号処理装置は、ＩＣカードである請求項６に記載の通信装置。

【請求項８】公開鍵および秘密鍵を有する公開鍵対を生成する鍵生成手段と、
秘密鍵を記憶する手段であって、要求に応じて前記生成された公開鍵対の秘密鍵により更新される秘密鍵記憶手段と、
前記生成された公開鍵対の公開鍵を、前記記憶されている秘密鍵を用いて暗号化する暗号化手段と、
前記秘密鍵を用いて暗号化された公開鍵を出力する出力手段とを有し、
前記生成された公開鍵対の秘密鍵および前記記憶されている秘密鍵は、外部に出力されない構成となっているＩＣカード。

【請求項９】平文が入力される入力手段をさらに有し、
前記暗号化手段は、さらに、前記入力された平文を、前記記憶されている秘密鍵を用いて暗号化して暗号文を生成し、
前記出力手段は、前記暗号化された暗号文を出力する請求項８に記載のＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、高いセキュリティ性で証明書の発行を行うことができ、これによりたとえばインターネットのようなオープンなネットワークを利

用してセキュリティ性の高い通信を行なうことができる通信システムおよび通信方法と、そのような通信システムを構築するのに好適な通信装置、および、そのような通信装置において鍵の管理に用いて好適なＩＣカードに関する。

【０００２】

【従来の技術】たとえば企業などにおいてローカルエリアネットワーク（ＬＡＮ）を構築する場合で、事業所が地理的に遠方の地に分散して存在するような場合には、各地区ごとに構築したＬＡＮを接続する必要がある。このような場合には、専用回線を用いてＬＡＮ同士を接続する場合が多い。しかしながら、近年では、たとえばインターネットのようなオープンなネットワークが既に構築され広く利用されており、このようなネットワークを介して前述したような各地区ごとのＬＡＮを接続することができれば、ＬＡＮの構築が容易になる上に通信コストが低減でき好適である。そこで、ＬＡＮ間接続をこのようなオープンなネットワークを介して行ない実質的に大規模なＬＡＮを構築するＶＰＮ（仮想内線網）なるシステムが提案されている。

【０００３】しかしながら、このようなオープンなネットワークシステムは、不特定多数の者が絶え間なく利用している上に、故意に不正なアクセスを試みる者も多数いることが予測され、セキュリティ性の点が大きな問題である。このような問題に対処するために、これまでのＶＰＮにおいては、接続対象のＬＡＮのゲートウェイ間で、認証局たるノードより発行される電子証明書を交換し、これにより通信相手の確認を行なうとともに暗号を用いるための鍵を交換し、以後暗号を用いて通信を行なうようにしている場合が多い。

【０００４】これまでの通信システムにおける、そのような電子証明書発行までの処理の流れを図３に示す。図３は、従来のＶＰＮのゲートウェイ間の認証処理の流れを模式的に示す図である。図３において、ゲートウェイ９０およびゲートウェイ２０は、各々特定のＬＡＮとインターネットを接続するゲートウェイであり、認証局３０はインターネット上の任意のノード上に設けられた機能である。

【０００５】なお、これらのゲートウェイ９０，２０および認証局３０における暗号化、認証、署名などの処理は、公開鍵と秘密鍵の鍵ペアを利用する公開鍵方式、より具体的にはＲＳＡ（Revest-Shamir-Adleman)方式により行なう。そして、ゲートウェイ９０には自分の公開鍵および秘密鍵からなるＲＳＡ鍵ペア（図中では、各々Ｖ溝を有するシンボルＡおよびＶ山を有するシンボルＡで示す）および認証局３０の公開鍵（図中では、Ｖ溝を有するシンボルＣＡで示す）が、ゲートウェイ２０には同じく自分の公開鍵および秘密鍵からなるＲＳＡ鍵ペア（図中では、各々Ｖ溝を有するシンボルＢおよびＶ山を有するシンボルＢで示す）および認証局３０の公開鍵が、認証局３０には自分の秘密鍵（図中では、Ｖ山を有するシンボルＣＡで示す）、ゲートウェイ９０の公開鍵およびゲートウェイ２０の公開鍵が、各々予め保持されているものとする。

【０００６】このような各ゲートウェイ９０，２０および認証局３０を有するＶＰＮ９において、ゲートウェイ９０とゲートウェイ２０の間で暗号を用いて通信を行なうためには、各ゲートウェイが自分の公開鍵を通信先のゲートウェイに送信する必要がある。そして、公開鍵の転送を行なう際には、各ゲートウェイにおいて本当に適切な相手から送信された鍵かどうかを判定する必要がある。そこで、各ゲートウェイ９０，２０は、自分の公開鍵を認証局３０に送って、認証して電子証明書を発行してもらい、その電子証明書を通信先に送信するようにしている。電子証明書を受信したゲートウェイにおいては、その電子証明書が適切に認証局３０で認証の行なわれたものであることを検査すれば、その電子証明書に含まれる公開鍵を適切な公開鍵と判定することができる。

【０００７】図３に示す構成に基づいて、この公開鍵の転送の処理およびそれに続く通信処理について具体的に説明する。まず、ゲートウェイ９０は、自分の公開鍵に対して自分の秘密鍵を用いて電子署名を行い、電子証明書の発行を認証局３０に要求する（①）。認証局３０は、この要求を受領したら、保持しているゲートウェイ９０の公開鍵を用いてこの電子署名の検査を行う。電子署名が適切、すなわち正当にゲートウェイ９０により行なわれたものであった場合には、認証局３０は、認証局３０の秘密鍵を用いてゲートウェイ９０の公開鍵に電子署名を行い、電子証明書としてゲートウェイ９０に返信する（②）。これを受け取ったゲートウェイ９０は、通信相手たるゲートウェイ２０にこの証明書を送信する（③）。ゲートウェイ２０はこの電子証明書を受け取ったら、保持している認証局３０の公開鍵を用いて、その電子証明書の署名の検査を行う。そして、署名が適切であれば、ゲートウェイ９０の公開鍵を保持する。

【０００８】同様に、ゲートウェイ２０は、自分の公開鍵に対して、自分の秘密鍵を用いて電子署名を行い、電子証明書の発行を認証局３０に要求する（④）。認証局３０は、この要求を受領したら、保持しているゲートウェイ２０の公開鍵を用いてこの電子署名の検査を行う。電子署名が適切、すなわち正当にゲートウェイ２０により行なわれたものであった場合には、認証局３０は、認証局３０の秘密鍵を用いてゲートウェイ２０の公開鍵に電子署名を行い、電子証明書としてゲートウェイ２０に返信する（⑤）。これを受け取ったゲートウェイ２０は、通信相手たるゲートウェイ９０にこの証明書を送信する（⑥）。ゲートウェイ９０はこの電子証明書を受け取ったら、保持している認証局３０の公開鍵を用いて、その電子証明書の署名の検査を行う。そして、署名が適切であれば、ゲートウェイ２０の公開鍵を保持する。

【０００９】このようにして公開鍵の交換が終了したら、ゲートウェイ９０およびゲートウェイ２０は、各々、通信文を自分が保持している自分の秘密鍵を用いて暗号化し、相手に送信する。これを受信したゲートウェイ２０およびゲートウェイ９０は、各々先に送信された相手の公開鍵用いてこれを復号し、元の平文の通信文を得る。このように、認証局３０を介して各ゲートウェイの認証を行なった上で、暗号を用いてゲートウェイ間で通信を行なうことにより、オープンなネットワークを用いたＬＡＮの接続を実用的なものとし、ＶＰＮを実現可能にしている。

【００１０】

【発明が解決しようとする課題】ところで、このような暗号処理、署名・認証処理など（以後、これらを全て含めて一般的に暗号という場合もある）においては、暗号化方式、暗号化アルゴリズムなどとともに、鍵の管理が非常に重要である。特に、前述した署名・認証や暗号に用いたＲＳＡ方式などの公開鍵方式においては、秘密鍵の管理が非常に重要である。

【００１１】しかしながら、前述した通信システムにおいては、その秘密鍵は、通常計算機システムなどで構成されるゲートウェイ上で生成され保持されているため、たとえば鍵生成の処理のオペレータやゲートウェイの管理者などゲートウェイに十分なアクセス権を有する者であれば、容易にこれを読み出すことができ、秘密鍵が漏洩する可能性があるという問題がある。その結果、通信システム全体のセキュリティ性を低下させることになり、たとえば前述したようなオープンなネットワークシステムを用いてＶＰＮなどのセキュリティ性の高い通信を行なおうとした時には、大きな問題となる。

【００１２】このような問題に対処するために、たとえば特開平９－２６１２１７号公報には、ＩＣカードなど外部より容易にアクセスすることのできない装置内で鍵を生成するという方法が提案されている。しかしながら、ＩＣカード内で鍵を生成したとしても、その鍵を用いて認証などの通信に係わる処理を行うのはゲートウェイ装置であり、また、少なくともＩＣカードより生成した鍵のデータを読み出す際にはデータとして読み出されるので、ゲートウェイの管理者など特権を有する者であれば、これを読み出せることに変わりはなく、セキュリティ性が十分とは言えない。

【００１３】したがって、本発明の目的は、たとえゲートウェイの管理者であっても、そのゲートウェイで管理する秘密鍵を読み出すことができず、認証処理や電子証明書の発行処理などをより高いセキュリティ性で行うことができ、これによりたとえばインターネットのようなオープンなネットワークを介してもセキュリティ性の高い通信を行なうことができる通信システムおよび通信方法を提供することにある。また、本発明の他の目的は、管理者であっても自らの管理する秘密鍵を読み出すことができず、種々の認証処理をより高いセキュリティ性で行うことができる通信装置を提供することにある。また、本発明の他の目的は、そのような通信装置に用いて好適な、秘密鍵を外部からアクセスされないように保持して認証・署名処理などを行なうことのできるＩＣカードを提供することにある。

【００１４】

【課題を解決するための手段】前記課題を解決するために、本発明の通信システムは、複数のノードおよび認証局が、必要に応じて相互の公開鍵を保持し、公開鍵方式に基づいた暗号文を用いて相互に通信を行なう通信システムであって、前記ノードの少なくとも１つのノードは、公開鍵および秘密鍵を有する公開鍵対を内部で生成し、秘密鍵は内部で外部よりアクセス不可能に保持し、生成した公開鍵を、以前に生成し内部に保持されている秘密鍵を用いて暗号化し出力する暗号処理装置と、前記暗号処理装置より出力された以前の秘密鍵を用いて暗号化された生成された公開鍵を、前記認証局に送信し、前記生成された公開鍵に前記認証局が認証を行なった電子証明書を獲得する電子証明書獲得手段と、前記獲得した電子証明書を、通信先のノードに送信し、公開鍵の更新を行なう送信手段とを有する。

【００１５】また、本発明の通信方法は、複数のノードおよび認証局が、必要に応じて相互の公開鍵を保持し、公開鍵方式に基づいた暗号文を用いて相互に通信を行なう通信方法であって、前記ノードの少なくともいずれかのノードにおいて、外部より任意にアクセス不可能な装置であって、公開鍵および秘密鍵を有する公開鍵対を内部で生成し、秘密鍵は内部で外部よりアクセス不可能に保持し、少なくとも生成した公開鍵を以前に生成し内部に保持されている使用中の秘密鍵を用いて暗号化し出力する暗号処理装置を用いて、使用中の秘密鍵を用いて暗号化された新たな公開鍵データを生成し、前記暗号化された新たな公開鍵データを前記認証局に送信し、前記認証局は、送信された前記暗号化された新たな公開鍵データを復号化して、該新たな公開鍵データを獲得し、前記獲得した新たな公開鍵データに当該認証局の秘密鍵を用いて認証を行ない、前記認証を行なった公開鍵データを当該公開鍵データの送信元のノードに送信し、当該送信元のノードは、前記認証局の認証の得られた公開鍵データを、通信先の任意のノードに送信し、前記認証局の認証の得られた公開鍵データが送信されたノードは、前記認証局の公開鍵を用いて前記認証の検査を行ない、前記新たな公開鍵を獲得し、前記送信元のノードと他のノードおよび認証局は、前記獲得された新たな公開鍵を用いて前記通信を行なう。

【００１６】好適には、前記送信元のノードは、任意のデータを送信する際には、当該データを前記暗号処理装置に入力し、当該暗号処理装置内において該データを前記内部に保持されている使用中の秘密鍵を用いて暗号化

し、当該暗号化したデータを送信先に送信する。

【００１７】また、本発明の通信装置は、複数のノードおよび認証局が、必要に応じて相互の公開鍵を保持し、公開鍵方式に基づいた暗号文を用いて相互に通信を行なう通信システムにおいて、前記ノードとして用いられる通信装置であって、公開鍵および秘密鍵を有する公開鍵対を内部で生成し、秘密鍵は内部で外部よりアクセス不可能に保持し、生成した公開鍵を、以前に生成し内部に保持されている秘密鍵を用いて暗号化し出力する暗号処理装置と、前記暗号処理装置より出力された以前の秘密鍵を用いて暗号化され生成された公開鍵を、所望の通信先に送信する通信手段とを有する。

【００１８】好適には、前記通信手段は、前記暗号処理装置より出力された以前の秘密鍵を用いて暗号化され生成された公開鍵を、まず前記認証局に送信し、前記生成された公開鍵に前記認証局が認証を行なった電子証明書を獲得し、さらに、前記獲得した電子証明書を、所望の通信先のノードに送信する。また好適には、送信対象のデータを前記暗号処理装置に入力する入力手段をさらに有し、前記暗号処理装置は、前記入力される送信対象のデータを、前記以前に生成し内部に保持されている秘密鍵を用いて暗号化し出力し、前記通信手段は、さらに、前記出力された暗号化された送信対象のデータを、所望の通信先のノードに送信する。特定的には、前記暗号処理装置は、ＩＣカードである。

【００１９】さらに、本発明のＩＣカードは、公開鍵および秘密鍵を有する公開鍵対を生成する鍵生成手段と、秘密鍵を記憶する手段であって、要求に応じて前記生成された公開鍵対の秘密鍵により更新される秘密鍵記憶手段と、前記生成された公開鍵対の公開鍵を、前記記憶されている秘密鍵を用いて暗号化する暗号化手段と、前記秘密鍵を用いて暗号化された公開鍵を出力する出力手段とを有し、前記生成された公開鍵対の秘密鍵および前記記憶されている秘密鍵は、外部に出力されない構成となっている。

【００２０】好適には、平文が入力される入力手段をさらに有し、前記暗号化手段は、さらに、前記入力された平文を、前記記憶されている秘密鍵を用いて暗号化して暗号文を生成し、前記出力手段は、前記暗号化された暗号文を出力する。

【００２１】

【発明の実施の形態】本発明の実施の形態を図１および図２を参照して説明する。本実施の形態においては、ＬＡＮ間をインターネットで接続したＶＰＮにおいて、ＬＡＮとインターネットを結合するゲートウェイ間でセキュリティ性を維持して通信を行なうための構成および方法を例示して、本発明を説明する。なお、本実施の形態において以下の説明の中で行なう暗号化、認証、署名などの処理は、公開鍵と秘密鍵の鍵ペアを利用する公開鍵方式、より具体的にはＲＳＡ（Revest-Shamir-Adleman）方式により行なうものとする。

【００２２】図１は、そのＶＰＮの特にＬＡＮ間接続部の構成を模式的に示すとともに、ゲートウェイ間で適切な通信を行なうための処理の流れを示す図である。ＶＰＮ１は、図１に示すように、ゲートウェイ１０、ゲートウェイ２０および認証局３０がインターネットにより接続されたものである。まず、ゲートウェイ１０、ゲートウェイ２０および認証局３０の構成について説明する。

【００２３】ゲートウェイ１０は、図示せぬ特定のＬＡＮとインターネットを接続するゲートウェイ（ルータ）である。ゲートウェイ１０は、実際には複数の通信ポートを有する計算機システムにより構成され、また、ＲＳＡ鍵の生成および署名処理を行なう本発明に係わるＩＣカード４０が装着されているものである。

【００２４】このようなゲートウェイ１０は、まず、自らがゲートとなっているＬＡＮから他のＬＡＮあるいはインターネット上の他のノードへの通信、および、他のＬＡＮあるいはインターネット上の他のノードから、自らがゲートとなっているＬＡＮへの通信を中継する。その際に、ゲートウェイ１０は、ＶＰＮ１を構成する他のＬＡＮへデータを送信する場合、換言すれば他のＬＡＮのゲートウェイへデータを送信する場合には、そのデータを自分の秘密鍵を用いて暗号化してインターネット上に送出する。また、ＶＰＮ１を構成する他のＬＡＮから送信されたデータを受信する、換言すれば他のＬＡＮのゲートウェイから送信されたデータを受信する場合には、そのデータは暗号化されているので、予め保持しているその送信元の公開鍵を用いてその受信データを復号化し、自らの管理するＬＡＮに送出する。

【００２５】また、ゲートウェイ１０は、前述したような中継処理を行なうために、通信相手の認証の処理を行なう。前述したように、他のＬＡＮのゲートウェイから送信されたデータを受信する場合には、そのゲートウェイの公開鍵を保持しておく必要がある。通常、この公開鍵は、最初の通信に先立ってネットワークを介して送信されてくるが、この公開鍵は、認証局３０による署名が行なわれた形態で送信されてくる。そこで、ゲートウェイ１０は、予め保持している認証局３０の公開鍵を用いてこの送信されてくる公開鍵が確かに認証局３０により認証を得ているものであるか否かの検査を行なう。検査に合格した公開鍵は、その通信先から送信されてくる暗号化された通信文の復号に用いる。

【００２６】また、ゲートウェイ１０は、逆に、新たな他のＬＡＮなどの通信先と通信を行なおうとした場合に、自分の公開鍵をその通信先に送信する処理を行なう。そのために、まずゲートウェイ１０は、自分の公開鍵を自分の秘密鍵で暗号化して認証局３０に送信し、公開鍵に対する署名の要求を行なう。そして、認証局３０より、ゲートウェイ１０の公開鍵に認証局３０による署名がなされた電子証明書が送信されてきたら、検査した

後、それを新たな通信先に送信する。新たな通信先において、この認証局３０による署名が検査され、ゲートウェイ１０の公開鍵が登録されれば、以後、その通信先に対して任意の情報を暗号化して送信することが可能となる。この時は、平文をゲートウェイ１０の秘密鍵を用いて暗号化を行なった通信文を送信することになる。

【００２７】さらに、ゲートウェイ１０においては、自分の公開鍵および秘密鍵の更新などの鍵の管理に係わる処理も行なう。暗号化処理や電子署名に用いる鍵は、通常、定期的に更新する必要がある。そのためゲートウェイ１０においては、定期的に公開鍵および秘密鍵からなる新たな公開鍵ペアを生成し、この新たな公開鍵を古い現在使用されている秘密鍵により暗号化して、認証局３０を始めとする通信先に配信する。これにより、ゲートウェイ１０の鍵ペアは、常にセキュリティ性が維持される。

【００２８】ゲートウェイ１０においては、このように種々の処理を行なうが、秘密鍵に係わる処理については、装着されているＩＣカード４０の内部で行なうようにしている。具体的には、通信文を秘密鍵を用いて署名をする処理、新たな鍵ペアを生成する処理、および、公開鍵に秘密鍵を用いて署名を行なう処理である。このような処理を行なうＩＣカード４０の構成および動作について、図２を参照し詳細に説明する。

【００２９】図２は、計算機システムに装着され、その計算機システムとともにゲートウェイ１０を構成するＩＣカード４０の構成を示すブロック図である。ＩＣカード４０は、ＲＳＡ鍵生成部４１、新公開鍵記憶部４２、新秘密鍵記憶部４３、現秘密鍵記憶部４４、署名部４５およびインターフェイス部４６を有する。

【００３０】まず、ＩＣカード４０の各部の構成について説明する。ＲＳＡ鍵生成部４１は、図示せぬ制御部からの制御信号に基づいて、公開鍵暗号方式、特にＲＳＡ方式による暗号化および復号化処理に用いる公開鍵のペア、すなわち、公開鍵と秘密鍵のペアを生成し、公開鍵は新公開鍵記憶部４２に、秘密鍵は新秘密鍵記憶部４３に出力する。

【００３１】新公開鍵記憶部４２は、ＲＳＡ鍵生成部４１より入力される新たに生成された公開鍵を記憶し、要求に応じて適宜署名部４５に出力する。

【００３２】新秘密鍵記憶部４３は、ＲＳＡ鍵生成部４１より入力される新たに生成された秘密鍵を記憶し、要求に応じて適宜現秘密鍵記憶部４４に出力する。

【００３３】現秘密鍵記憶部４４は、現在ゲートウェイ１０が暗号化、署名処理において使用している秘密鍵を記憶し、要求に応じて適宜署名部４５に出力する。現秘密鍵記憶部４４に記憶されている秘密鍵は、ゲートウェイ１０が使用する鍵を更新する時に、新秘密鍵記憶部４３に記憶されている新たな秘密鍵が現秘密鍵記憶部４４に読み込まれることにより、更新される。

【００３４】署名部４５は、新公開鍵記憶部４２より入力される新たに生成された公開鍵、あるいは、後述するインターフェイス部４６より入力される通信平文に対して、現秘密鍵記憶部４４に記憶されている秘密鍵を用いて、所定の暗号化アルゴリズムにより署名を行ない、インターフェイス部４６に出力する。

【００３５】インターフェイス部４６は、ＩＣカード４０とＩＣカード４０が装着されている計算機システムとの信号の送受を行なうためのインターフェイス部である。ＩＣカード４０は、所定の信号に定義された８つの電極を有する接触式のＩＣカードであってリーダ／ライタ装置に装着されて用いられる。インターフェイス部４６は、この電極を介して、所定の通信プロトコルにより、リーダ／ライタ装置を介して、外部計算機システムと通信を行なう。

【００３６】具体的には、署名部４５で秘密鍵により署名された公開鍵または通信文のデータが、インターフェイス部４６を介してゲートウェイ１０の本体たる外部計算機システムに出力される。また、外部計算機システムからは、署名対象の通信平文がインターフェイス部４６を介して署名部４５に入力される。また、ＩＣカード４０内の図示せぬ制御部と、外部計算機装置の制御信号の伝送も、このインターフェイス部４６を介して行なわれる。

【００３７】なお、ＩＣカード４０は図示せぬ制御部を有している。この制御部が、インターフェイス部４６を介して外部計算機システムと通信を行なうことにより、外部計算機システムからＩＣカード４０に対して処理の命令などが行なわれる。また、この命令に基づいて、制御部は、ＩＣカード４０の全体が協働して所望の処理を行なうように、ＩＣカード４０の各部を制御する。

【００３８】このような構成のＩＣカード４０の動作について説明する。まず、ゲートウェイ１０が鍵ペアを更新する場合にＩＣカード４０が係わる処理について説明する。その場合、通常はまず、外部計算機システムからＩＣカード４０に対して、新たなＲＳＡ鍵ペアの生成が指示される。これによりＩＣカード４０では、ＲＳＡ鍵生成部４１においてＲＳＡ鍵ペアを生成し、公開鍵は新公開鍵記憶部４２に、秘密鍵は新秘密鍵記憶部４３に各々記憶する。

【００３９】また、外部計算機システムより生成した新たな公開鍵を秘密鍵で署名したデータが要求された場合には、ＩＣカード４０は、新公開鍵記憶部４２に記憶している新たな公開鍵を署名部４５に出力し、署名部４５で現秘密鍵記憶部４４に記憶されている現在の秘密鍵を用いてこの新たな公開鍵に署名を行ない、この署名の行なわれた公開鍵をインターフェイス部４６を介して外部計算機システムに出力する。

【００４０】次に、ゲートウェイ１０が送信する通信平文に署名を行なう処理について説明する。この場合、外

部計算機システムよりインターフェイス部４６を介して通信平文が入力されるので、インターフェイス部４６はこれを署名部４５に入力し、署名部４５で現秘密鍵記憶部４４に記憶されている秘密鍵を用いて署名を行ない、再びインターフェイス部４６を介して外部計算機システムに戻す。

【００４１】ＩＣカード４０は、外部計算機システムからの指示に応じてこのような処理を行なう。

【００４２】ゲートウェイ２０も、ゲートウェイ１０と同様に、図示せぬ特定のＬＡＮとインターネットを接続するゲートウェイであり、その構成、動作などは、ゲートウェイ１０と実質的に同じである。

【００４３】認証局３０は、インターネット上の任意のノード上に設けられ、各ゲートウェイに対して種々の認証処理を行なう。本発明に係わる処理としては、認証局３０は、ゲートウェイ１０およびゲートウェイ２０からの要求に基づいて、ゲートウェイ１０およびゲートウェイ２０が送信してきた各公開鍵の検査を行い、その公開鍵が確かにゲートウェイ１０およびゲートウェイ２０のものであることを証明する電子証明書を発行する処理を行なう。

【００４４】次に、このようなゲートウェイ１０、ゲートウェイ２０および認証局３０を有するＶＰＮ１の動作、処理の流れについて説明する。まず、初期状態として、ゲートウェイ１０には自分の公開鍵および秘密鍵からなるＲＳＡ鍵ペア（図中では、各々Ｖ溝を有するシンボルA_1およびＶ山を有するシンボルA_1で示す）および認証局３０の公開鍵（図中では、Ｖ溝を有するシンボルＣＡで示す）が、ゲートウェイ２０には同じく自分の公開鍵および秘密鍵からなるＲＳＡ鍵ペア（図中では、各々Ｖ溝を有するシンボルＢおよびＶ山を有するシンボルＢで示す）および認証局３０の公開鍵が、認証局３０には自分の秘密鍵（図中では、Ｖ山を有するシンボルＣＡで示す）、ゲートウェイ１０の公開鍵およびゲートウェイ２０の公開鍵が、各々予め保持されているものとする。

【００４５】このような状態において、まず、ゲートウェイ１０が使用する鍵を更新する処理について説明する。その場合、まずゲートウェイ１０の計算機システムは、装着されているＩＣカード４０に対して新たなＲＳＡ鍵ペアの生成を要求する（①）。ＩＣカード４０では、これに基づいて、ＲＳＡ鍵生成部４１でＲＳＡ鍵ペアを生成し、公開鍵（図中では、Ｖ溝を有するシンボルA_2）を新公開鍵記憶部４２に、秘密鍵（図中では、Ｖ山を有するシンボルA_2）を新秘密鍵記憶部４３に記憶する。新たな鍵の生成が終了したら、計算機システムは、ＩＣカード４０に対して、現在の秘密鍵で署名を行なった新たな公開鍵を要求する。その結果、ＩＣカード４０においては、署名部４５において、新公開鍵記憶部４２に記憶されている新たな公開鍵が、現秘密鍵記憶部４４に記憶されている現在用いられている秘密鍵を用いて署名され、インターフェイス部４６を介して計算機システムに送信される（②）。

【００４６】このようにして得られた現秘密鍵により署名された新公開鍵は、ゲートウェイ１０より認証局３０に送信され、認証局３０に新公開鍵が通知されるとともに、新公開鍵に対する電子証明書の発行が要求される（③）。認証局３０においては、ゲートウェイ１０の現公開鍵を用いて送信された内容を検査し、確かにゲートウェイ１０から送信されたものであること確認すると、その新たなゲートウェイ１０の公開鍵を記憶しておく。また、自分（認証局３０）の秘密鍵によりゲートウェイ１０の新公開鍵に署名を行なって電子証明書を作成し、ゲートウェイ１０に送信する（④）。ゲートウェイ１０においては、送信された電子証明書を、認証局３０の公開鍵を用いて検査し、確かに認証局３０により作成された電子証明書であることを確認する。

【００４７】この電子証明書を入手したら、ゲートウェイ１０は、ゲートウェイ２０を含む各通信先にこの電子証明書を送信し、新たな公開鍵を通知する（⑤）。この電子証明書を受信したゲートウェイ２０などの各通信先においては、認証局３０の公開鍵を用いて受信した電子証明書を検査し、適切に認証局３０で認証の行なわれたものであることを確認して、その電子証明書に含まれるゲートウェイ１０の新公開鍵を抽出し登録する。このように、ゲートウェイ１０の新たな公開鍵は、認証局３０およびゲートウェイ２０を含む各通信先に送信される。そして、ゲートウェイ１０が何らかの手段により通知した鍵の切り換えタイミングにより、ゲートウェイ２０および認証局３０など各通信先においてゲートウェイ１０との通信で用いる鍵を切り換え、また、ゲートウェイ１０においても、新秘密鍵記憶部４３に記憶されている秘密鍵を現秘密鍵記憶部４４に転送するなどして使用する鍵の変更処理を行なえば、鍵の更新が行なわれたことになる。

【００４８】以後、ゲートウェイ１０が新たな通信先に自分の公開鍵を送信する場合などは、既に認証局３０より得ている電子証明書を送信すればよい。また、ゲートウェイ２０も、同様に方法により適宜鍵の更新を行なうものである。

【００４９】次に、このようなＶＰＮ１において、実際にデータの送信を行なう場合の処理について説明する。ゲートウェイ１０が、自分のＬＡＮのノードからの通信平文をゲートウェイ２０のＬＡＮに含まれるノードに送信する場合、ゲートウェイ１０の計算機システムは、まずその通信平文を、ＩＣカード４０に送信し、秘密鍵による署名を指示する（⑥）。ＩＣカード４０においては、この通信平文をインターフェイス部４６を介して署名部４５に入力し、署名部４５において、この通信平文に現秘密鍵記憶部４４に記憶されている秘密鍵を用いて署名

を行ない、インターフェイス部４６を介して再び計算機システムに返信する（⑦）。そして、このようにして署名の行なわれた通信文が、ゲートウェイ１０よりゲートウェイ２０に送信される（⑧）。ゲートウェイ２０においては、ゲートウェイ１０の公開鍵を用いて受信した通信文を平文に戻し、自分のＬＡＮ内の所望のノードに送信する。

【００５０】このように、本実施の形態のＶＰＮ１の特にゲートウェイ１０においては、自分の鍵といえども、秘密鍵に係わる処理は、生成から使用、更新まで、全てＩＣカード４０内で行なわれており、ＩＣカード４０外部へは解析可能な形で全く出力されていない。したがって、たとえばゲートウェイ１０の管理者と言えども、この秘密鍵を知ることは実質的に不可能であり、秘密鍵をより安全に保管することができ、ひいては、ゲートウェイ１０、ＶＰＮ１の信頼性が向上する。

【００５１】

【発明の効果】このように、本発明によれば、たとえゲートウェイの管理者であっても、そのゲートウェイで管理する秘密鍵を読み出すことができず、認証処理や電子証明書の発行処理などをより高いセキュリティ性で行うことができ、これによりたとえばインターネットのようなオープンなネットワークを介してもセキュリティ性の高い通信を行なうことができる通信システムおよび通信方法を提供することができる。また、管理者であっても自らの管理する秘密鍵を読み出すことができず、種々の認証処理をより高いセキュリティ性で行うことができる通信装置を提供することができる。さらに、そのような通信装置に用いて好適な、秘密鍵を外部からアクセスされないように保持して認証・署名処理などを行なうことのできるＩＣカードを提供することができる。

【図面の簡単な説明】

【図１】図１は、本発明の一実施の形態の通信システムであるＶＰＮの、特にＬＡＮ間接続部の構成を模式的に示すとともに、ゲートウェイ間で適切な通信を行なうための処理の流れを示す図である。

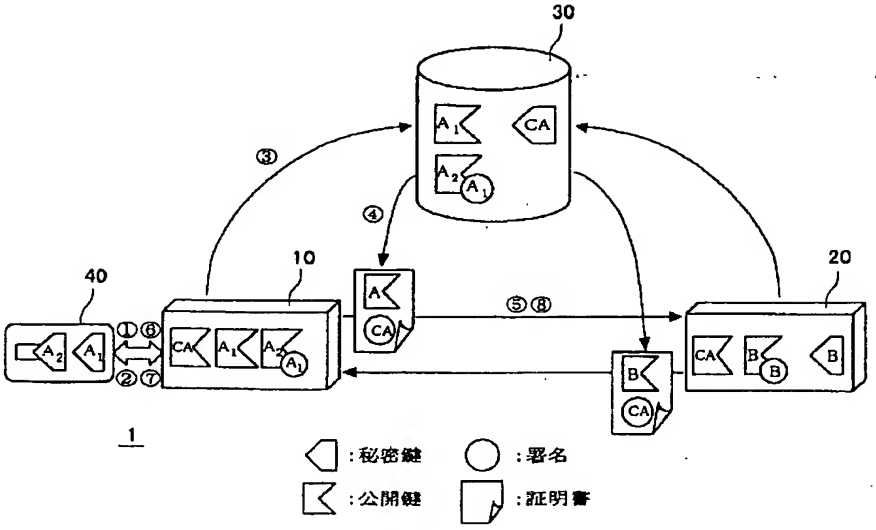
【図２】図２は、図１に示したＶＰＮのゲートウェイにおいて計算機システムに装着して用いられるＩＣカードの構成を示すブロック図である。

【図３】図３は、従来のＶＰＮにおける、ＬＡＮ間接続部の構成およびゲートウェイ間での処理の流れを示す図である。

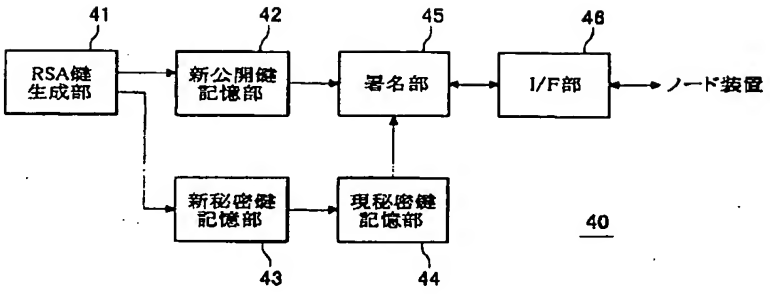
【符号の説明】

１、９…ＶＰＮ
１０，２０，９０…ゲートウェイ
３０…認証局
４０…ＩＣカード
４１…ＲＳＡ鍵生成部
４２…新公開鍵記憶部
４３…新秘密鍵記憶部
４４…現秘密鍵記憶部
４５…署名部
４６…インターフェイス部

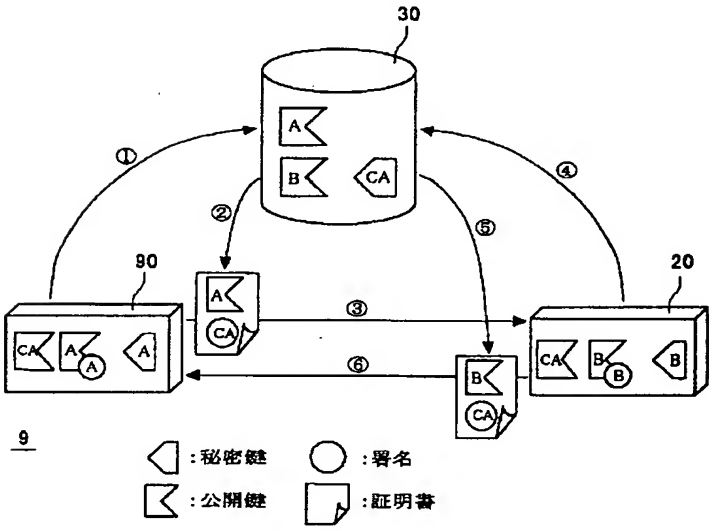
【図１】



【図２】


41
42
45
46
RSA鍵
生成部
新公開鍵
記憶部
署名部
I/F部
ノード装置
新秘密鍵
記憶部
現秘密鍵
記憶部
40
43
44

【図３】


30
A
B
CA
①
②
③
④
⑤
⑥
90
20
CA
A
A
CA
B
B
9
:秘密鍵
:署名
:公開鍵
:証明書